



FortiWLM

Release 8.3.1

FortiWLM 8.3.1 release includes important fixes to be patched on the FortiWLM 8.3.0 GA and this release notes is to be used as an addendum to the 8.3.0 GA release notes.



To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Fixed Issues

Bug ID	Description
0413853	Fixed infections reported by Microsoft Endpoint Protection when FortiWLM upgrade file is downloaded.

Common Vulnerabilities and Exposures

FortiWLM 8.3.1 is no longer vulnerable to the following CVE-Reference:

- 2017-7336
- Visit <https://fortiguard.com/psirt> for more information

Known Issues and Limitations

Bug ID	Description	Work Around
398408	WIPS UI not accessible in fresh install of FortiWLM for the first time.	Reboot FortiWLM server. After reboot, WIPS would be accessible.
423960	FortiWLC-SD 1000D/3000D 8.3.0 controllers cannot be upgraded from FortiWLM since SFTP is not supported on FortiWLC-SD	Upgrade using FortiWLC-SD GUI/CLI.

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the [local contact numbers](#), or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet® and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable